Appl. No.: 09/879,849
Amdt. Dated: 06/15/2004
Off. Act. Dated: 01/15/2004

REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested in view of the foregoing amendments and discussion presented herein.

1. Claim Objections.

Claims 7, 12 and 13 were objected to as having ambiguous step numbering. A form of replacement step numbering was suggested.

Claims 7 and 13. The Applicant has amended Claim 7 and Claim 13 according to the Examiner's suggestions.

Claim 12. This claim was previously canceled in the preliminary amendment filed June 11, 2001. Therefore, the objection is moot with regard to Claim 12.

2. Rejection of Claims 1, 3-9, 11, 13-21, 24-25 and 28 under 35 U.S.C. § 103(a).

Claims 1, 3-9, 11, 13-21, 24-25 and 28 were rejected as being unpatentable under 35 U.S.C. § 103(a) to Matsumoto et al. (US Pat. No. 5,465,299).

After carefully considered the grounds for rejection, the Applicant responds as follows. Prior to discussing specific claim rejections, it should be understood that Matsumoto et al. '299 describes a method that allows one party (A) to create a signed document D and then have additional parties (B, C, ...) modify the document and add their own signatures to the modified document (D', D", ...). Matsumoto et al. '299 is not concerned with the cryptographic details of forming a given digital signature by a given party.

However, this approach is not the approach described in the application or recited in the claims. The objects of the invention differ, the principles of operation differ, and the structures of the inventions are incompatible. The Applicant does not describe a multi-signatory signature scheme nor any method by which an original document D is being modified to a new document D'. There is just the one document that is being signed in the Applicant's invention.

(a) Claims 1, 19, 24. These independent claims were considered to read on the method of signing a data string. Specifically the rejection states: "*a) hashing the data*

string and a seed (salt) value to generate a hash value reads on Fig. 2A, elements 106 for the hash value, additional data area 103 as the seed or salt value and the fixed data area 102 as the data string; b) encoding into an image point the hash value, the seed value and a given portion of the data string reads on signature data 107 comprising a subregion number for the seed or salt value, hash total of document data for the hash value and the given portion of the data string for the personal information 110; and c) applying a given decryption primitive to the image point to obtain a digital signature of the data string reads on the encipher process 112 and resulting digital signature 113C."

The *"additional data area 103"* of Matsumoto et al. '299 was considered to equate to *"the seed or salt value"* as recited in the claims. However, this is an incorrect interpretation of the meaning of *"additional data area 103"*, which cannot be equated to a seed or salt value. Specifically, the *"additional data area 103"* is described in Matsumoto et al. at column 6, lines 17-21: *"document 101 which is sequentially circulated to a plurality of users comprises: a fixed data area 102 in which the change of the contents is not permitted; and an additional data area 103 into which data is added at the terminal on the circulating destination side."*

The additional data area 103 therefore provides an area accessible in which content and notes are entered from parties that receive the document after the original drafter. The content and notes can be of varying length and content, and typically would comprise notes, such as editing comments. These are not used in the signatory process of the original document, but are included to support the multi-signatory mechanism that Matsumoto et al. teaches. Furthermore, the contents of data area 103 does not equate to a *"seed"* as specified in the claims by the Applicant. A seed is of a fixed length for a given signature scheme and is chosen at random with no humanly meaningful semantics. The seed therefore is something internal to the signing process, it is used to make the signing process more secure, not to add functionality, such as the additional information that is added in the process of Matsumoto et al. whose intent is to incrementally encode data as the document is passed along. Furthermore, the seed is

not associated with an incremental or multiple signatory process, which is the only purpose of data area 103 in the teachings of Matsumoto et al. '299.

Regarding Claim 1, since Matsumoto et al. '299 does not teach a process of *"encoding into an image point the hash value, the seed value, and a given portion of the data string"*, as recited in Applicant's Claim 1, it does not anticipate that claim. It should be noted that Claim 19 and 24 provide additional limitations concerning the seed which were not considered in the rejection. This *seed* element is not taught by Matsumoto et al. '299, wherein Claim 1 cannot be considered as being anticipated by that reference.

Regarding Claim 19, which describes further information about the *"seed"*, and specifically recites *"means for hashing the data string and a random seed value to generate a keyed value"* and further describes *"means for encoding into an image point the keyed hash value, the random seed value and a given portion of the data string"*.

In these elements the seed has been further recited as being a *"random seed value"* and is described being used in the hashing means and the encoding means. Applicant respectfully submits that neither of these limitations were addressed in the rejection, and neither of these limitations were taught by Matsumoto et al. '299. Consequently, Claim 19 cannot be considered as being anticipated by that reference.

Regarding Claim 24, it is seen that this independent claim adds further limitations to the *"seed"* described in Claim 1 and Claim 19. Specifically, the claim recites: *"(a) selecting a random seed r; (b) hashing the data string and the random seed r to generate a hash value h(r,M); (c) encoding into an image point y the hash value h(r,M), the random seed r, and the second portion M2 of the data string; (d) applying a decryption primitive to the image point y to obtain a digital signature x of the data string; wherein the random seed r is selected so that the image string y is in the domain of the decryption primitive."*

The Applicant respectfully submits that the rejection does not address *"selecting a random seed"*, *"hashing the data string and random seed"*, *"encoding into an image point y the hash value h(r,M), the random seed r"*, nor does it address the selection of

the random seed being *"so that the image string y is in the domain of the decryption primitive"*. None of these elements are taught by Matsumoto et al. '299, wherein Claim 24 cannot be considered as being anticipated by that reference.

(b) Claims 11 and 17. These independent claims were rejected on the basis of: *"reading on the recovery portions 208, 209, 210 and the authentication process in general at 207 in Fig. 3"*.

These independent claims include limitations regarding the use of a *random seed* value which is not addressed in the rejection of these claims. Applicant respectfully submits that the rejection improperly focuses only on select additional elements found in Claims 11 and 17, and does not address all limitations of these claims. The traversal of the rejection in reference to the *"seed"* value limitation has already been described above with regard to independent Claims 1, 19, 24, and applies similarly here as well.

Furthermore, Applicant respectfully submits that indicating that *"Claims 8, 11, 13, 14, and 17 read on the recovery portions 208, 209, 210, and the authentication process in general at 207 in Fig. 3"* does not constitute proper support for the rejection as it does not indicate which elements of the claim are considered to correspond to what elements in the cited reference - only a generalized similarity of concept can be inferred.

However, even that generalized concept does not read on Claim 11 and 17 as nothing in relation to Fig. 3 in Matsumoto et al. describes recovery and authentication utilizing the random seed *r*, and therefore can also not describe the process of using that random seed which is given in detail within Claim 11 and 17. Furthermore, as previously mentioned the data area of Matsumoto et al. is used for containing comments and information from parties which receive the document along its review path, wherein this area is only associated with the incremental signature aspect of the Matsumoto et al. teaching, it does not describe how the original signatory of the document is formed.

Appl. No.: 09/879,849
Amdt. Dated: 06/15/2004
Off. Act. Dated: 01/15/2004

Regarding Claim 11, the claim describes in the preamble the signing and authentication of a data string M having two parts M1 and M2. The elements of the claim then continue on detailing the underlying method, and includes *"hashing the data string and a random seed r to generate a hash value h(r,M)"* as well as *"encoding into an image point y the hash value h(r,M), the random seed r, and the second portion M2 of the data string"* none of these elements are taught by the relied-upon Matsumoto et al. reference. As these elements do not exist within the Matsumoto '299 reference, the claims are not anticipated by that reference.

Regarding Claim 17, the preamble first breathes life into the claim describing the makeup of the digital signature which was *"generated by applying a given decryption primitive to an image point y, the image point y comprising a function of a seed value r, a hash value h(r,M), and a given portion of the data string"*. The steps within the method then operate based on that digital signature structure and address other aspects relating to the seed value, such as *"decoding the candidate image point to generate candidate values corresponding to the seed value r, the hash value h(r,M), and the given portion of the data string"*. As these elements are not addressed at all in the teachings of Matsumoto et al., and furthermore are not described in the relationships recited in Claim 17, they are not anticipated by the cited reference.

Claim 18. Although rejected on the basis of 35 U.S.C. 102, no grounds for rejection were provided in support of anticipation (or for any other rejection) of this claim. Claim 18 contains limitations which further describe the use of the seed value and other aspects to which no descriptions within the Matsumoto et al. reference have been discussed. Therefore, since these aspects are nowhere found in that reference, Claim 18 should be considered patentable and the unsupported rejection withdrawn.

Claims 20 and 21. Similarly, although these claims were rejected on the basis of 35 U.S.C. 102, no grounds for rejection based on anticipation (or for any other reason) were asserted against these dependent claims, which depend from a base claim shown to be allowable.

Claims 3-9, 13-16, 20-21, 23, 25 and 28. These claims depend from base claims which have been shown to be patentable, therefore, these claims should be considered *a fortiori* allowable.

Although these claims should be considered allowable in view of their dependence on claims shown to be allowable, many of these dependent claims contain elements which are patentably distinct in their own right, for example with regard to Claim 7. Claim 7 is a dependent claim which is said to read on the *"hashing of document 105 within the additional area 103"*. However, this dependent claim describes a step utilizing the *seed value*, the *seed value* not being taught in the relied upon reference, and certainly the use of seed value being *"concatenated"* to the data string is not taught. Many of the other claims also add details for which no teaching was found in the relied-upon Matsumoto et al. reference, even when considered separately.

Therefore, it has been shown that elements recited within independent Claims 1, 11, 17, 18, 19, 24 were not found in the relied-upon reference, wherein these claims are not anticipated by the reference. As a result, Applicant respectfully submits that the rejection of Claims 1, 11, 17, 18, 19, 24, along with the claims which depend therefrom, should be immediately withdrawn.

3. Claims 1, 3-11, 13-21, 23-25 and 28 are nonobvious.

Nor would the subject matter of Claims 1, 3-11, 13-21, 23-25 and 28 be obvious to a person having ordinary skill in the art in view of the Matsumoto et al. '299 reference.

Establishing a *prima facie* case of obviousness requires that some teaching, suggestion, incentive or motivation is found in the reference for modifying the reference to meet all limitations recited in Applicant's claims. The Matsumoto et al. reference is directed at different purposes, with different objectives, and it uses different operating principles to arrive at that intention. Matsumoto '299 describes a multiple signature scheme, and does not even teach the use of the seed values which are important

aspects of Applicant's invention. Further, there is no teaching within the reference that one of ordinary skill in the art would consider to be teaching, suggestion, motivation or incentive for modifying the reference toward the Applicant claims, the reference cannot be used as a primary reference in an obviousness rejection against these claims.

Therefore, since there is no suggestion, teaching, or motivation which can be found in the references from which a person of ordinary skill in the art would find it obvious to modify this reference to correspond with the apparatus of the Applicant; and further, since this reference is not even capable of being combined, claims 1, 3-11, 13-21, 23-25 and 28 recite structure which is patentable over the cited references for purposes of 35 U.S.C. § 103.

4. Traversal of Rejection of Claims 18 and 19; In re Donaldson.

The Applicant respectfully traverses the grounds for rejection of Claims 18 and 19, and cites *In re Donaldson*, 16 F.3d 1189, 1193 (Fed. Cir. 1994)(en banc) as the basis for the traversal. Claims 18 and 19 are written in means-plus-function form pursuant to 35 U.S.C. §112, sixth paragraph, and therefore, must be interpreted during examination under *In re Donaldson*.

In rejecting Claims 18 and 19, as well as the claims that depend therefrom, the Examiner made no specific fact findings as to the scope of equivalents for the means-plus-function elements in the claims. (Actually, with regard to Claim 18, no support is provided whatsoever for the rejection.) Instead, the Examiner appears to have followed the provisions of MPEP § 2183 ("Making a Prima Facie Case of Equivalence"), which states:

> If the examiner finds that a prior art element performs the function specified in the claim, and is not excluded by any explicit definition provided in the specification for an equivalent, the examiner should infer from that finding that the prior art element is an equivalent, and should then conclude that the claimed limitation is anticipated by the prior art element. The burden then shifts to applicant to show that the element shown in the prior art is not an equivalent of the structure ... disclosed in the application. *In re Mulder*, 716 F.2d 1542, 219 U.S.P.Q. 189 (Fed. Cir. 1983). No further analysis of equivalents is required of the examiner until applicant disagrees with the

examiner's conclusion, and provides reasons why the prior art element should not be considered an equivalent.

While the Examiner appears to have followed the provisions of MPEP §2183, such provisions are contrary to Federal Circuit law. The Federal Circuit has held that an examiner "construing means-plus-function language in a claim must look to the specification and interpret that language in light of the corresponding structure ... described therein, and equivalents thereof," *In re Donaldson*, 16 F.3d 1189, 1193 (Fed. Cir. 1994)(en banc), and in so ruling expressly denied that "the PTO is exempt from this mandate." Id. The Federal Circuit added that it was specifically overruling any precedent that suggested or held to the contrary. Id. at 1193-94. In response to the PTO's argument that the court's ruling conflicted with the principle that a claim should be given its broadest reasonable interpretation during prosecution, the Federal Circuit held that the Donaldson decision was setting "a limit on how broadly the PTO may construe means-plus-function language under the rubric of 'reasonable interpretation.'" Id. at 1194. In other words, an examiner's claim interpretation is not "reasonable" if it is not based on the specification's description of the implementation of the means element of the claim. The court then said, "Accordingly, the PTO may not disregard the structure disclosed in the specification corresponding to such [means-plus-function] language when rendering a patentability determination. " Id. at 1195.

Here, as in *Donaldson*, the Examiner is required by statute to look to the Applicant's specification and construe the "means" language as referring to corresponding means disclosed in the specification and equivalents thereof." See id. at 1195. However, the Examiner did not construe the means language of these claims. Nor did the Examiner find, on the basis of specific facts of record here, that the means disclosed in the Applicant's specification were equivalent to that of the cited references. Instead, as prescribed by MPEP §§ 2183-84, the Examiner simply presumed equivalence. The presumption methodology used here, which the MPEP prescribes, clearly conflicts with the requirements of the Federal Circuit's Donaldson decision. The

approach taken by the Examiner in this case also conflicts with *In re Bond*, 931 F.2d 831 (Fed. Cir. 1990).

The very point of these cases is that, in this context, limitations from the specification control the interpretation of the claim. Under §112, paragraph 6, a means-plus-function element of a claim must be construed to mean that which is disclosed in the specification and its equivalents. In *Donaldson*, the Federal Circuit said that "our holding does not conflict with the general claim construction principle that limitations found only in the specification of a patent or patent application should not be imported or read into a claim." In other words, the court was saying that a §112, paragraph 6 "means" element does not need to be "imported or read into" a means-plus-function claim because the specification's limitations and their equivalents are already in the claim by virtue of §112, paragraph 6's command. Thus, the Federal Circuit said (16 F.3d at 1195): "What we are dealing with in this case is the construction of a limitation already in the claim in the form of a means-plus-function clause and a statutory mandate on how that clause must be construed."

Based on the foregoing, the Applicant respectfully submits that the rejection of Claims 18 and 19, as well as the claims that depend therefrom lacks proper foundation and that the rejection should be withdrawn. Those claims, each of which include means plus function limitations, should have been interpreted in view of the specification as required by *In re Donaldson*. If those claims had been so interpreted, they would have been allowable since the cited references do not, singly or in combination, teach, suggest or provide motivation or incentive for the subject matter recited in those claims.

5. Rejection of Claims 2, 10, 12, 22-23, and 26-27 for statutory Double Patenting.

Claims 2, 10, 12, 22-23, and 26-27 were rejected for statutory double patenting as being unpatentable over claims 1-27 of U.S. Patent No. 6,266,771.

Claims 2, 12, 22, 26-27. These claims were cancelled by the Applicant's preliminary amendment filed with the application.

Appl. No.: 09/879,849
Amdt. Dated: 06/15/2004
Off. Act. Dated: 01/15/2004

Claims 10 and 23. The Applicant respectfully notes that the Examiner did not provide any information about the how these claims were considered to be coextensive in scope with any of the claims in U.S. Patent No. 6,266,771, wherein the Applicant has had to rely on making assumptions as to what aspects of these claims the Examiner based the rejection.

Applicant respectfully submits that these claims do not recite the same subject matter found in the claims in U.S. Patent No. 6,266,771. In both cases the Examiner appears to be comparing the dependent claim in isolation, without considering its reliance on the independent claim which clearly recites a different set of elements and scope than those issued in U.S. Patent No. 6,266,771. These defects in the rejection are addressed specifically as follows.

Referring to Claim 10, it is readily seen that although claim 10 contains the same wording as Claim 9 in the '771 patent, the claims to which these depend are written with obviously different scopes. Both claims depend from an independent Claim 1 in their own respective application, and these claims differ. Specifically, it is seen that Claim 1 of the '771 patent contains sublimits (i) and (ii) which are not present in Claim 1 in the instant application. Therefore, Claim 10 is not coextensive in scope with claims within the '771 patent.

Referring to Claim 23, it should first be noted that Claim 23 was amended as part of the preliminary amendment included with the filing of the continuation application. The wording for this claim is presented below for your convenience.

23. (previously presented): The computer program product as described in Claim 19 wherein the given function is an output of a generator applied to the keyed hash value.

Claim 23 of the instant case depends from Claim 19. In patent '771 claim 18 depends from Claim 15 and has similar wording to that of Claim 23. However, the scope of the dependent claim cannot be considered separately from the claims upon which it depends, and the base claims in the instant application and the parent case

differ in limitations and in scope. Specifically, Claim 15 of patent '771 contains the additional limitation within the second means element of: *"wherein the means for encoding includes means for masking the random seed value and, optionally, the given portion of the data string, using a given function;"*. As this limitation is not found in the base claim, Claim 19, of the instant application, and no interceding claims provide this limitation, Claim 23 is not coextensive with claims found in parent patent 6,266,771.

Therefore, Applicant respectfully submits that no support exists for the statutory double patenting rejection, wherein the rejection should be withdrawn.

6. Amendment of Claims 7, 13 and 25.

Claim 7. This claim was amended according to Examiner directive, wherein "step (a)" was replaced with "step 1(a)".

Claim 13. This claim was amended according to Examiner directive, wherein "step (h)" was replaced with "step 13(h)".

Claim 25. This claim was amended to correct the step lettering which was incorrectly given as step (d), although a step (d) was already given in the claim depended upon. Therefore step (d) was amended to indicate step (e).

7. Extension of time under 37 CFR 1.136(a).

A petition is enclosed for a two-month extension as described in 37 CFR 1.136(a); an appropriate fee is enclosed.

//

//

//

//

//

//

//

//

Appl. No.: 09/879,849
Amdt. Dated: 06/15/2004
Off. Act. Dated: 01/15/2004

8. Conclusion.

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to withdraw the outstanding rejection of the claims and to pass this application to issue.

The Applicant also respectfully requests a telephone interview with the Examiner in the event that there are questions regarding this response, or if the next action on the merits is not an allowance of all pending claims.

Date: June 15, 2004

Respectfully submitted,

John P. O'Banion, Reg. No. 33,201
Rodger H. Rast, Reg. No. 45,853
O'BANION & RITCHEY LLP
400 Capitol Mall, Suite 1550
Sacramento, CA 95814
(916) 498-1010